REMARKS

Applicant acknowledges with thanks the Examiner's indication that claims 6-9, 13-15, 17 and 27 would be allowable if rewritten in independent form to include all the limitations of the base claims and the intervening claims.

The Examiner maintained the rejection of claims 2-3, 24-26 and 32-40 as being unpatentable over "RFC 2977 -- Mobile IP Authentication, Authorization and Accounting Requirements" (RFC 2977) in view of U.S. Patent Application Publication No. 2002/0065785 to Tsuda and further in view of U.S. Patent No. 6,751,459 to Lee *et al.*

Applicant's independent claim 2 recites "receiving, by a receiver, a message from subscriber's user equipment, said message indicating that an address of a certificate provisioning gateway for certificate issuance and delivery procedure in a visited network is requested by the subscriber's user equipment, the certificate provisioning gateway serving at least one certificate authority, the message further containing the address of the certificate provisioning gateway; obtaining, by a processor, in response to receiving the message, subscriber's location information maintained in a mobile communication system; determining, by the processor, on the basis of the subscriber's location information, an address of the certificate provisioning gateway; checking, by the processor, whether or not the address of the certificate provisioning gateway received in the message is the same as the address of the certificate provisioning gateway determined on the basis of the location information; and when they are not the same, using, by the processor, the address determined on the basis of the location information."

Thus, the address of a certificate provisioning gateway that a subscriber's equipment is to access is determined from the subscriber's location information, and a determination is then made as to whether the address obtained matches the gateway's address specified in the received message. If there is a discrepancy between the two addresses, the address of the certificate provisioning gateway determined based on the subscriber location information is used.

In his rejection of independent claim 2, the Examiner admitted that "[RFC 2977] **is silent on use** of location information AND if they <u>are not the same</u>, using the address determined on the basis of the location information" (Emphasis in the original, Final Action, page 5). Thus, as acknowledged by the Examiner, RFC 2977 fails to disclose or suggest at least the features of "checking, by the processor, whether or not the address of the certificate provisioning gateway received in the message is the same as the address of the certificate provisioning gateway determined on the basis of the location information; and when they are not the same, using, by the processor, the address determined on the basis of the location information," as required by applicant's independent claim 2.

The Examiner, however, relies on Tsuda and Lee in support of the rejection of claim 2, and states:

> *As previously put forth in earlier rejections,* **Tsuda** teaches a network using Mobile IP and AAA protocols for general authentication and Accounting (eg. for a certificate issuance service in another network than a home network. See figure 10 shows mobile user registering with a foreign agent in a non-home network. Abstract and figure 1 show a system that allows a user to be authenticated to roam to various networks and use services whereby AAA information is transmitted to/from a user's device. Also see figure 6, Step 2 and figure 10 which shows an authentication procedure and figure 1 0 shows overall procedure whereby data is sent to/from the mobile's AAA-HIAAA-V servers in order to authenticate said user as he roams. Figures 10-1 1 show mobile authenticating with AAA and P#l86 discusses use of certificate issuance via certificate authority. Furthermore, he also teaches a Mobile IP network, figure 1 shows a mobile user who has roamed from a home network #l 001/#1010 to a visited network #l 002/#1010 connected via IP which inherently subnets a network into smaller networks and their location is known based on where the engineer has positioned the local access router1BTS. Lastly, the mobile network maintains user location in an HLR and Tsuda teaches both home and foreign networks, P#67 and P#71, which inherently describes the concept of *knowing where the user is (eg. maintaining a subscriber's location in the network)* since it is either in the (one) home network or in any of other foreign networks -- see figure 18 which shows multiple foreign subnets, #l 002/#1004. Tsuda clearly shows multiple networks connected each having an AAA/Certificate server (figures 1-2). Hence a de-centralized AAA server design would inherently require the user's authentication request to be handled by the "local" AAA server. Figure 3 shows a connection from AAA #70 to AAA #60 on different networks with a "broker" in between (reads on a CA Provisioning Gateway). Also see figure 6 which shows that the two networks/AAA's interact, steps 101-109. With regard to using geographical position data to assist with network configuration/authentication, Lee teaches an "automated process" to enable nomadic roaming such that a user can request connectivity to a device whereby an agent determines the user has roamed into a visited network and translates the request into a connection to a new, similar device (Abstract). This alleviates the need for the user to track/determine if they have roamed into a visited network and then request a new device address. Furthermore, Lee puts forth multiple connected networks that use various services from the different networks. One skilled understands that a network design would either be centralized or distributed. Thusly, the AAA/Certificate servers would either all be at one location or spread out across the network -- forcing the user to either always contact the central server or contact a local server. Figure 4 clearly shows that the user uses both voice and data services and that the network tracks the user across multiple networks (See Care-of-Address and various TID's). Therefore the use of one or multiple

> "certificate authorities" is viewed as a **design choice.** (Emphasis in the original, Final Action, pages 6-7)

Applicant respectfully disagrees with the Examiner's contentions.

Tsuda describes a mobile communication system containing mobile node devices according to the Mobile IP protocol and an AAA server device for supporting the mobile node devices according to the AAA protocol (Tsuda, page 1, paragraph 2). In relation to Tsuda's FIG. 11, showing a sequence for a registration/authentication and accounting operations in the communication system involving interactions between the AAA systems of two networks, Tsuda explains:

> **[0088] When the mobile node 1010 receives the advertisement packet, this received advertisement packet and the earlier received advertisement packet are compared, and when it is judged that the IP address of the subnet has changed, in order to detect the moving between the subnets and carry out the registration of the Mobile IP protocol, that is, in order to register the care-of address (such as FA (Foreign Agent) care-of address provided by the foreign agent 1021 or the co-located care-of address obtained by the DHCP or the like at the home agent 1011, the mobile node transmits the registration request packet containing that address to the foreign agent 1021 (step S102).**
>
> **[0089] Note that the registration request packet from the mobile node 1010 is assumed to contain an identification information (e-mail address, for example) called NAI (Network Access Identifier), and an mn-aaa authentication expanded portion including the authentication information.**
>
> **[0090] When the foreign agent 1021 receives the above described registration request packet, if it is a new registration request, the foreign agent 1021 inspects the challenge field and checks whether it is the challenge value sent by the foreign agent 1021 itself or not is checked. When it is judged that it is the challenge value sent by the foreign agent 1021 itself, the foreign agent 1021 transmits the above described registration request packet to the AAAF server 1022 for carrying out the authentication and accounting processes regarding the communication fee of that subnet (step S103).**
>
> **[0091] When the AAAF server 1022 receives the above described registration request packet, if it is a new registration request, the AAAF server 1022 creates a new entry, and transfers the above described registration request packet to the AAAH server 1012 (step S104). Note that the AAAF server 1022 can identify the AAAH server 1012 of the home network of the mobile node 1010 from the NAI stored in the registration request packet.**
>
> **[0092] When the AAAH server 1012 receives the above described registration request packet, the AAAH server 1012 checks a portion called MN-AAA auth. of this packet, and when it is judged that the authentication is success as a result of this check, the AAAH server 1012 creates an entry for the mobile node 1010, generates a home IP address to be used by the mobile node 1010, and produces a first key to be**

> **used between the mobile node 1010 and the home agent 1011 and a second key to be used between the mobile node 1010 and the foreign agent 1021. Then, the AAAH server 1012 transmits the registration request packet containing the home IP address and the first key to the home agent 1011 (step S105), and returns the registration response packet containing the home IP address, the first key and the second key to the mobile node 1010 (step S106).**
>
> **[0093] The home agent 1011 and the mobile node 1010 carries out the necessary registration and setting according to the above described packets from the AAAH server 1012. In this way, the mobile node 1010 becomes capable of carrying out communications as a mobile node according to the Mobile IP, and the accounting process for the communication fee will be carried out.**
>
> **[0094] Now, in the registration request packet, a life time is described. In order to continue the communication using the Mobile IP, the mobile node 1010 transmits the second or subsequent registration request packet to the home agent 1011 before the life time is over. (Tsuda, pages 6-7, paragraphs 88-94)**

Thus, through the interaction sequence depicted in FIG. 11, a mobile unit sending a registration request packet receives a registration response request containing a home IP address, a first key to be used between the mobile unit and a home agent, and a second key to be used between the mobile node and the foreign agent (see in particular paragraph 92). Tsuda, however, does not describe that a mobile unit sends a message that includes location information and an address of a certificate provisioning gateway, nor does Tsuda describe that any system determines the address of a foreign certificate provisioning gateway based on the location of the mobile node and determines if the determined address and the address in the message received from the mobile node match. Accordingly, Tsuda fails to disclose or suggest at least the features of "checking, by the processor, whether or not the address of the certificate provisioning gateway received in the message is the same as the address of the certificate provisioning gateway determined on the basis of the location information; and when they are not the same, using, by the processor, the address determined on the basis of the location information," as required by applicant's independent claim 2.

Lee describes a method and apparatus for supporting nomadic computing of a personal mobility system with transparent virtual networking, information storage, and mobility when the user is traveling from one location to another and/or using different computer platforms or operating modes (Lee, col. 1, lines 14-20). Lee explains that:

> **To overcome the shortcomings of the prior systems, among other shortcomings, the present invention provides a method and apparatus for nomadic computing by means of transparent virtual networking, information storage, and mobility when**

> **the user is traveling from one location to another and/or using different computer platforms or operating modes. Personal mobility domain name service (PMDNS) is originally designed to provide personal mobility via a personal identifier. Because of generic system architecture which uses the Internet as backbone, interoperating with existing access networks, it is also wise to provide nomadic computing services.**
>
> **To accomplish such operations, a personal mobility directory server is updated with information concerning a user's nomadicity. When the user travels from one place to another, the user registers with a PMDNS server at an IP port for computing communications. The PMDNS employs the user's terminal personalization together with a usage profile and session characteristics to map a party's identifier to a terminal's identifier. The IP address of the user's current location can be used in concert with the terminal's identifier, which is in itself an IP address, to route incoming computing communications connection requests to the current location of the user. This information is returned by the PMDNS directory server to the access network for the setup of the communications. (Lee, col. 2, line 49 to col. 3, line 7)**

Lee does not describe, however, making a determination if a certificate provisioning gateway at a visited network at which a user's equipment is located, determined from location information of the user's equipment, matches an address of the certificate provisioning gateway provided by a message sent by the user's equipment. Accordingly, Lee too fails to disclose or suggest at least the features of "checking, by the processor, whether or not the address of the certificate provisioning gateway received in the message is the same as the address of the certificate provisioning gateway determined on the basis of the location information; and when they are not the same, using, by the processor, the address determined on the basis of the location information," as required by applicant's independent claim 2.

Because none of the references cited by the Examiner discloses or suggests, alone or in combination, at least the features "checking, by the processor, whether or not the address of the certificate provisioning gateway received in the message is the same as the address of the certificate provisioning gateway determined on the basis of the location information; and when they are not the same, using, by the processor, the address determined on the basis of the location information," applicant's independent claim 2 and the claims depending from it are patentable over the cited art.

Applicant's independent claims 3, 24-26 and 32-35, recite "receiving, by a receiver, a message from subscriber's user equipment, the message containing subscriber's location information and indicating that an address of a certificate provisioning gateway for certificate issuance and delivery procedure in a visited network is requested by the subscriber's user equipment, the certificate provisioning gateway serving at least one certificate authority; obtaining, by a processor, in response to receiving the message, subscriber's location information maintained in a mobile communication system; checking, by the processor, whether or not the subscriber's location information received in the message corresponds to the subscriber's location information obtained; and using, by the processor, the subscriber's location information obtained to determine the address of the certificate provisioning gateway when the subscriber's location information obtained does not correspond to subscriber's the location information received in the message," or similar language.

Thus, independent claims 3, 24-26 and 32-35 require a determination of whether information provided in a message (e.g., subscriber's location) sent by the subscriber's equipment matches information independently determined by a processor receiving the subscriber's message. On the basis of that determination, an address of a certificate provisioning gateway in the visited network may be provided.

Accordingly, for reasons similar to those provided with respect to independent claim 2, the cited art fails to disclose at least the features of "checking, by the processor, whether or not the subscriber's location information received in the message corresponds to the subscriber's location information obtained; and using, by the processor, the subscriber's location information obtained to determine the address of the certificate provisioning gateway when the subscriber's location information obtained does not correspond to subscriber's the location information received in the message," or similar language, as required by applicant's independent claims 3, 24-26 and 32-35. Applicant's independent claims 3, 24-26 and 32-35, and the claims depending from them are therefore patentable over the cited art.

CONCLUDING COMMENTS

It is believed that all of the pending claims have been addressed in this paper. However, failure to address a specific rejection, issue or comment, does not signify agreement with or concession of that rejection, issue or comment. In addition, because the arguments made above are not intended to be exhaustive, there may be reasons for patentability of any or all pending claims (or other claims) that have not been expressed. Finally, nothing in this paper should be construed as an intent to concede any issue with regard to any claim, except as specifically stated in this paper, and the amendment of any claim does not necessarily signify concession of unpatentability of the claim prior to its amendment. Applicant asks that all claims be allowed.

If there are any questions regarding these amendments and remarks, the Examiner is encouraged to contact the undersigned at the telephone number provided below. The Commissioner is hereby authorized to charge any additional fees that may be due, or credit any overpayment of same, to Deposit Account No. 50-0311, Reference No. 39700-583001US / NNC37029-US-NP.

Respectfully submitted,

Date: July 22, 2009

Ido Rabinovitch

Ido Rabinovitch
Reg. No. L0080

Address all written correspondence to
Mintz, Levin, Cohn, Ferris, Glovsky and Popeo, P.C.
One Financial Center
Boston, Massachusetts 02111
Customer No. 64280
Telephone: 617-348-1806
Facsimile: 617-542-2241